Notice of Allowability	Application No.	Applicant(s)	
	09/930,836	KOCHER ET AL.	
	Examiner	Art Unit	
	Justin T. Darrow	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *a request for continued examination filed 09/10/2004*.

2. ☒ The allowed claim(s) is/are *41-50*.

3. ☒ The drawings filed on *15 August 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1-50 have been presented for examination. Claims 1-40 have been cancelled and new claims 41-50 have been added in a preliminary amendment filed 08/15/2001. Claims 41-50 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 09/10/2004 has been entered.

Priority

3. Acknowledgment is made that the instant application is a continuation of Application No. 09/324,798, filed 06/03/1999, which has the benefit of the earlier filing date of provisional Application No. 60/087,826, filed 06/03/1998.

Information Disclosure Statement

4. The information disclosure statements (IDSes) submitted on 07/28/2005, 04/28/2005, 12/31/2004, 12/21/2004, 11/03/2004, 09/30/2004, and 09/10/2004 were filed before the mailing date of a first Office after the filing of a request for continued examination under 37 CFR 1.114

on 09/10/2004. The submission is in compliance with the provisions of 37 CFR 1.97(b)(4). Accordingly, the information disclosure statements are being considered by the examiner.

Allowable Subject Matter

5. Claims 41-50 are allowed.

6. The following is an examiner's statement of reasons for allowance:

Claims 41-46 are drawn to a method for performing a cryptographic operation. The closest prior art, Markham, U.S. Patent No. 5,796,836 A, discloses a similar method.

Markham illustrates a method for performing a cryptographic operation, where the cryptographic operation includes performing a substitution operation using a predefined substitution table (see column 5, lines 8-18; figure 2b, item 36; the encryption module uses a substitution box which uses a vector), comprising:

(a) obtaining a representation of a predefined substitution table specifying a corresponding table value for each of a plurality of possible table index values (see column 5, lines 26-31; figure 1d, item 12; a codebook for a DES encryption algorithm);

(b) using random information, transforming the representation of the predefined substitution table into a new randomized representation of the substitution table (see column 6, lines 27-30; figure 2b, items 32 and 34; pseudorandom vectors generated by the codebook module); and

(c) receiving datum to be cryptographically processed (see column 6, lines 32-33; plaintext to be encrypted).

However, Markham neither teaches nor suggests:

(d) computing a blinded representation of a table index value from at least the datum;

(e) using the new randomized representation of the table, performing a substitution on the blinded table index to derive a blinded representation of the table index value to derive a blinded representation of the table value corresponding to an unblended version of the table index value in step (d); and

(f) using the blinded table value to compute a cryptographic result for use in securing a cryptographic protocol.

The preamble is a limitation because the method step of claim 41 requires the manipulation of particular structures that are identified by the preamble, during a particular sequence of events defined only by the preamble. See MPEP § 2111.02 and *Eaton Corp. v. Rockwell International Corp.*, 66 USPQ2d 1271, 1277 (Fed. Cir. 2003).

This combination of limitations explicitly recited in independent claim 41 renders claims 41-46 allowable.

Claim 47 is drawn to a method for performing a cryptographic operation. The closest prior art, Markham, U.S. Patent No. 5,796,836 A, discloses a similar method.

Markham illustrates a method for performing a cryptographic operation involving a substitution operation using a predefined substitution table (see column 5, lines 8-18; figure 2b, item 36; the encryption module uses a substitution box which uses a vector), comprising:

(a) obtaining random information (see column 5, lines 56-60; cryptographic modes which employ a cryptographic algorithm output (pseudorandom vector) register (e.g., cipher feedback and output feedback));

(b) using random information, producing a randomized representation of a table (see column 6, lines 27-30; figure 2b, items 32 and 34; pseudorandom vectors generated by the codebook module); and

(c) receiving datum to be cryptographically processed (see column 6, lines 32-33; plaintext to be encrypted).

However, Markham neither teaches nor suggests:

(d) applying the randomized representation of the table to a table input derived from at least the datum to produce a substitution result randomized by the random information;

(e) using the randomized result, deriving a cryptographic result, where the cryptographic result is independent of the random information; and

(f) using the cryptographic result as part of securing a cryptographic protocol.

The preamble is a limitation because the method step of claim 47 requires the manipulation of particular structures that are identified by the preamble, during a particular sequence of events defined only by the preamble. See MPEP § 2111.02 and *Eaton Corp. v. Rockwell International Corp.*, 66 USPQ2d 1271, 1277 (Fed. Cir. 2003).

This combination of limitations explicitly recited in independent claim 47 renders this claim allowable.

Claims 48-50 are drawn to a device for performing a cryptographic operation. The closest prior art, Markham, U.S. Patent No. 5,796,836 A, discloses a similar device.

Markham shows a device for performing a cryptographic operation, comprising:

(a) a source of random data (see column 5, lines 56-60; cryptographic modes which employ a cryptographic algorithm output (pseudorandom vector) register (e.g., cipher feedback and output feedback));

(b) table randomized logic configured to use an output from the source of the random data (see column 6, lines 27-30; figure 2b, items 32 and 34; pseudorandom vectors generated by the codebook module); and

(c) a memory for storing a randomized representation of a predefined substitution table (see column 6, lines 2-4; figure 2b, item 34; the pseudorandom vectors are stored in output FIFO module).

However, Markham neither teaches nor suggests:

(d) table input parameter computation logic, configured to produce a table input parameter from at least a portion of an input message and the output from the source of random data;

(e) first cryptographic computation logic, configured to produce a table input parameter from at least a portion of an input message and the output from the source of random data; and

(f) second cryptographic logic, configured to use the first cryptographic computation logic to compute a cryptographic result, where the cryptographic result depends solely on the key and the input message and is independent of the output from the source of random data.

This combination of features explicitly incorporated in independent claim 48 renders claims 48-50 allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is 571-273-8300. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers

transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to 571-273-8300 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

August 21, 2005

Justin Darrow

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100